

Análisis de ciberataque a la UES usando Inteligencia de fuentes abiertas.

Jimmy Anthony Hernández Umaña.

26 de mayo del 2021

Introducción

“The university is as bad as the university / For a better education”**(1)**, ésta leyenda apareció en un fondo negro en el sitio https://biblioteca.ues.edu.sv el día 11 de julio del año 2020, anunciando así que la seguridad del sitio había sido comprometida, es un típico ejemplo de un *deface* web, un término que hace referencia a modificar de forma no autorizada un sitio de terceros para dejar un mensaje y firma del autor del acto vandálico, en este caso la firma que se encontró en el sitio se atribuye a un pirata informático llamado “C0RT3X”, adicionalmente también se vio afectado el sistema de registro académico “PROMETEO”.

Resumen

Esta investigación recopila información obtenida de distintas fuentes de datos para hacer una serie de correlaciones sobre la identidad de este pirata informático “C0RT3X”, entre ellas utilizando parámetros avanzados de búsqueda de google, sitios web, búsqueda inversa de imágenes, servicios de consulta de filtraciones de datos, registros históricos de defaces, notas periodísticas y finalmente redes sociales como Facebook.

En el desarrollo de la misma se logró localizar a una persona que utiliza el pseudónimo “C0RT3X” y se le realizó una entrevista en la cual se abortaron temas sobre su *modus operandi*, además de su participación en un grupo llamado “Pacman Corp” y sobre su supuesta participación en el suceso.

Finalmente se llegó a una conclusión que apunta a una suplantación de identidad y un acto de sabotaje de alguien motivado con fines políticos.

Planteamiento del problema

El ciberataque provocó una interrupción en las labores de la universidad y puso en riesgo la privacidad y seguridad de los registros de las personas inscritas en el sistema, ¿Quién es el autor o autores del ataque? ¿Cuál es la motivación de el mismo? ¿Cuál fue el efecto del mismo?

Antecedentes

No existen antecedentes de una investigación que se haya hecho pública acerca de este u otro ciberataque hacia la infraestructura de la Universidad de El Salvador.

Aun así no es la primera vez que la universidad recibe algún tipo de acto de vandalismo similar, por ejemplo en el sitio web www.zone-h.org/archive que se dedica a documentar defaces web, existe el registro de al menos 17 ocasiones desde el año 2005 en las cuales ha ocurrido.

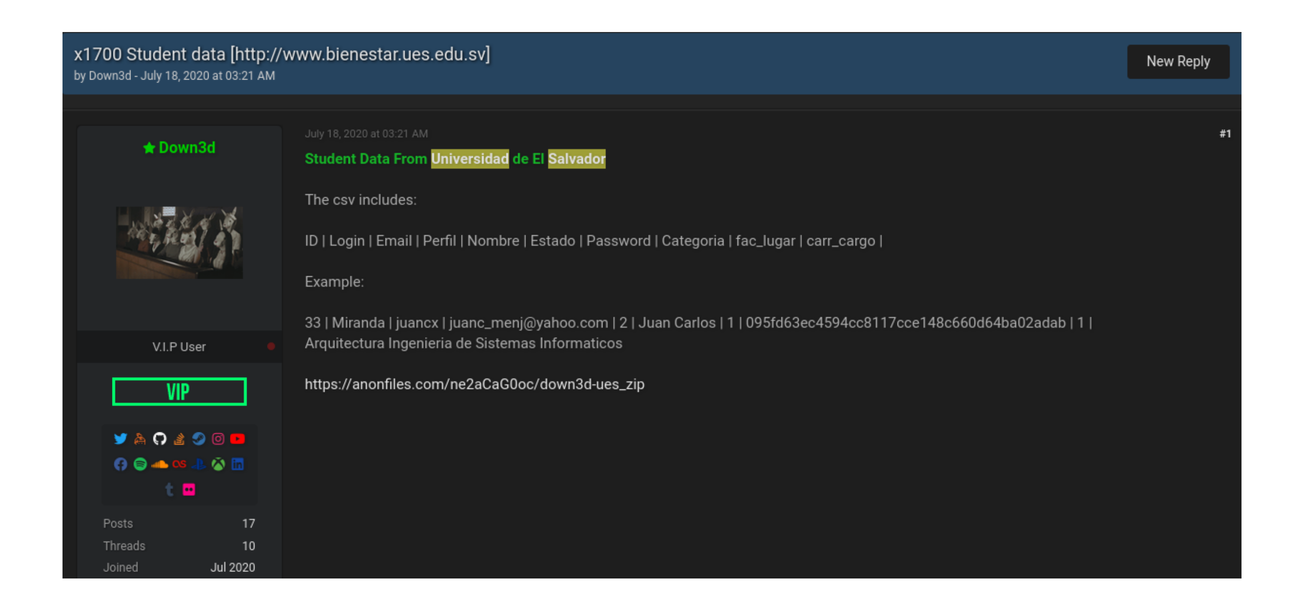
Total notifications: **17** of which **10** single ip and **7** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2020/06/13	KingSkrupellos						minerva.sic.ues.edu.sv/public/...	Linux	mirror
2018/05/08	Mr-Cakil		M				www.congresohistoria.humanidad...	Linux	mirror
2018/05/08	Mr-Cakil		M				www.academica.humanidades.ues....	Linux	mirror
2018/05/08	Mr-Cakil		M				www.postgrados.humanidades.ues...	Linux	mirror
2018/05/08	Mr-Cakil		M				www.secretaria.humanidades.ues...	Linux	mirror
2018/05/08	Mr-Cakil		M				www.periodismo.humanidades.ues...	Linux	mirror
2018/04/27	Electronic Thunderbolt Team						proyeccion.social.agronomia.ue...	Linux	mirror
2018/04/25	Mr-Cakil						www.quimicayfarmacia.ues.edu.s...	Linux	mirror
2018/04/25	Mr-Cakil		M				www.odontologia.ues.edu.sv/sit...	Linux	mirror
2018/04/20	jok3r		M				academica.cimat.ues.edu.sv/133...	Linux	mirror
2018/04/20	h0d3_g4n						icmares.cimat.ues.edu.sv/toch.txt	Linux	mirror
2017/08/01	CyBeRiZM						revistas.ues.edu.sv/public/sit...	Linux	mirror
2015/04/16	Laakel En Person	H					www.uese.ues.edu.sv	Linux	mirror
2015/01/19	MexicanHackers						www.genero.ues.edu.sv/x.txt	Linux	mirror
2014/09/14	Index Php						chagasecosalud.censalud.ues.ed...	Linux	mirror
2014/04/14	Moroccan Hassan						www.defensoria.ues.edu.sv//ima...	Linux	mirror
2005/11/25	byond hackers team	H					www.matematica.ues.edu.sv	Linux	mirror

Además en un foro de discusión anglosajón de intercambio de filtraciones de datos se hizo pública la información de 1,700 estudiantes registrados en http://www.bienestar.ues.edu.sv, esto sucedido el día 18 de julio del 2020 y no existe ningún comunicado oficial al respecto.

https://raidforums.com/Thread-x1700-Student-data-http-www-bienestar-ues-edu-sv?highlight=Universidad+de+El+Salvador



Aparte de eso existe un mercado negro de credenciales y accesos robados que ofrece a la venta dos accesos a paneles de administración del sistema de correos de la universidad solicitando como medio de pago bitcoin, lastimosamente estos acontecimientos exceden a los objetivos de este documento y no se entrará en detalle con ellos.

Delimitación del problema

Los hechos a estudiar en la investigación comprenden desde el 11 de julio del 2020 al 12 de julio del mismo año, ocurrió en el subdominio de la universidad https://biblioteca.ues.edu.sv/ y el sistema PROMETEO de la misma, afectando el cambio de notas del ciclo 1-2020, dado el funcionamiento de internet el ataque pudo haber sido realizado de cualquier parte del mundo, aunque se da por supuesto que existe la probabilidad que el autor o autores del hecho sean de nacionalidad Salvadoreña.

Justificación

La realización y publicación de este reporte es importante porque no se ha realizado una similar acerca de lo sucedido, es necesario identificar a los responsables dado que es una acción maliciosa que pone en riesgo la integridad de la institución y de la seguridad personal de los estudiantes dado el contenido de información privada que se aloja en sus servidores, es necesario dar seguimiento a las amenazas de la red tanto como las físicas dado estamos en una era de la información y el internet se ha vuelto parte de nuestra vida diaria.

Objetivos

Objetivo general:

Analizar la información obtenida con fuentes abiertas para entender el contexto en el cual se realizó el ciberataque.

Objetivos específicos:

- Desanonimizar la identidad detrás del pseudónimo de C0RT3X.
- Encontrar posibles motivaciones del ciberataque.
- Comprobar si el ataque fue organizado por un actor interno.
- Obtener toda la información posible que tenga correlación con lo sucedido.
- Procesar la información obtenida para luego analizarla de forma crítica.
- Rastrear a el autor/autores del ataque utilizando la información analizada.
- Descartar posibles hipótesis acerca del ataque.

Hipótesis

Toda acción tiene una causa, toda causa tiene un efecto, esto es algo que siempre se debe tener en cuenta a la hora de analizar un ciberataque, en este caso tenemos dos tipos diferentes, por una parte un defacement y por otro una modificación a un sistema de base de datos, los motivos de un defacement, que viene a ser como un grafiti digital suelen ser políticos, religiosos o en la mayor parte de los casos por diversión de los hackers que se dedican a hacer la mayor cantidad de defaces posibles para ganar fama acumulando “trofeos” y suelen dejar imágenes, frases y su firma en el sitio alterado para que todos sepan quién lo modificó

Los defaces hechos por personas que dedican a hacerlos como pasatiempo no hacen ataques dirigidos, suelen ser al azar buscando vulnerabilidades en servidores de internet, pero sin profundizar en ellos, lo cual puede apuntar a que los motivos de éste ataque no fué realizado por alguien por diversión, sino con otros motivos, personas que podrían beneficiarse del suceso, ya sea de forma económica o política, siendo en ese entonces una época de gran tensión social/política en El Salvador por el manejo de la pandemia, el manejo de fondos públicos y los conflictos entre distintos órganos del gobierno.

El día siguiente se publicó un comunicado oficial en el cual se sugiere que este ataque es motivado por la posición ante la deuda presupuestaria de $13,000,000 y por “otras opiniones respecto al contexto de la realidad nacional”, la verdad es que esas son acusaciones sarcásticas muy extrañas, no tiene sentido que el gobierno intente desestabilizar una institución pública como lo es la UES.

https://twitter.com/UESoficial/status/1282396252567744513/photo/1

Expuesto el contexto es posible que el responsable sea alguien interno, que busque influenciar políticas o económicamente la situación de la universidad.

Marco Teórico

Existe una vasta documentación acerca del tema de los defacements, según Luis Diago de Aguilar *«Defacement es un ataque a un sitio web que cambia la apariencia visual de una página web. Normalmente son producido por "hackers" (no no no, ciberdelincuentes) que obtuvieron algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.»* ***(2)***

Motivaciones

Desde Trendmicro nos exponen una serie de motivaciones que un atacante puede tener a la hora de realizar un deface:

Los atacantes pueden tener diferentes motivaciones cuando alteran un sitio web. La motivación política es una. Los atacantes que están en contra de un gobierno o un movimiento en particular pueden optar por alterar los sitios web relacionados para ventilar sus puntos de vista. Los atacantes que hacen esto se conocen como "hacktivistas". Pueden cambiar el contenido del sitio web alterado con una imagen o un mensaje de su elección.

Otros atacantes pueden optar por alterar un sitio web por diversión, para burlarse de los propietarios del sitio al encontrar vulnerabilidades del sitio web y aprovecharlas para alterar el sitio web. Estos atacantes "se burlan" de los propietarios del sitio. Al igual que los hacktivistas, estos atacantes alteran un sitio web con una imagen o un mensaje de su elección. (traducido) **(3)**

Vectores de Ataque

Cuando nos referimos a vectores de ataque hacemos alusión a formas en las que un atacante puede comprometer un sistema informático y lograr alterar el contenido del sitio web, el INCIBE**(4)** (Instituto de Ciberseguridad) hace un listado de los mismos:

- Robo de credenciales de acceso mediante malware enviado por correo electrónico.
- Explotación de vulnerabilidades en gestores de contenido desactualizados con plugins antiguos o mal configurados.
- Servidores web infectados por malware o ataques realizados a través de dominios alojados en el mismo servidor ya comprometido.

Ciberamenazas en relación a las universidades

El **Estudio de Ciberseguridad en el sector universitario** llevado a cabo por Deloitte**(5)**, según el cual el 80% de las universidades participantes declararon haber sufrido algún incidente en los últimos 12 meses. De ellas, el 62% ha sufrido entre 2 y 5 ciberataques y el 10% recibió más de 10. Estos datos vienen a ilustrar la creciente preocupación que existe actualmente en las organizaciones por sus posibles efectos, y que han motivado que las ciberamenazas hayan escalado a las posiciones más altas de los mapas de riesgos de las empresas, de forma que son monitorizados cada vez más de cerca por los Consejos de Administración.

Consecuencias de Ciberataques

Se reporta mediante el informe The State of Cybersecurity and Digital Trust 2016 realizado por Accenture**(6)**   que durante el año 2016 un 69% de las empresas ha sufrido algún robo o intento de robo de datos, usualmente los ataques buscan simplemente dañar sus

infraestructuras, extorsionar a las empresas como por ejemplo usando rasomware y forzar a las víctimas a pagar grandes sumas para tener acceso a la información secuestrada por los piratas informáticos y finalmente tenemos el robo directo; referente a la sustracción de información confidencial o propiedad intelectual.

En el artículo "Qué consecuencias puede tener un ciberataque para tu empresa" del blog Reasonwhy**(7)** se definen distintas consecuencias directas de un ciberataque:

Pérdida de datos

Los ataques cibernéticos normalmente giran en torno al robo de información sensible como investigaciones, estrategias empresariales, informes financieros… Las bases de datos digitales también están en el punto de mira de los hackers. Perder esta información puede, literalmente, conducir a la ruina a muchas empresas.

Y es que, en muchas ocasiones, las empresas que más cantidad de datos manejan son sometidas a la extorsión de los ciberdelincuentes. Los hackers piden grandes cantidades de dinero a cambio de no atacar los sistemas corporativos o de dejar de hacerlo.

Desembolso económico

Bien sea por extorsión; bien sea por los costes de reparación y limpieza de las infraestructuras afectadas, un ciberataque siempre conlleva un desembolso económico para la empresa.

Y la merma es más acusada cuando se trata de empresas pequeñas, porque no sólo tienen que hacer frente al coste de recuperar los datos robados, sino también a la posible pérdida de clientes; la fuga de empleados, que se sienten más inseguros tras el ciberataque; y el coste de instalar nuevos sistemas de seguridad en la empresa (cambio de contraseñas, nuevo antivirus…). También hay que contar con los costes de reestructuración en caso de que, a raíz de un hackeo, se haya contratado plantilla extra.

Cambio en el modelo de negocio

El cibercrimen puede tener consecuencias para las empresas más allá del aspecto financiero. Algunas llegan a replantearse la forma en la que recopilan los datos y la información de sus clientes, para asegurarse de que ésta no vuelva a ser vulnerable.

De hecho, muchas empresas optan por no volver a almacenar los datos personales y financieros de sus clientes, tales como tarjetas de crédito o fecha de nacimiento.

En el caso de los e-commerce, algunos han llegado a cerrar el site por su incapacidad para hacer frente a este tipo de ataques masivos. Y es que los clientes hoy en día son muy celosos de su privacidad y no confían sus datos financieros a aquellas empresas que tienen fallos de seguridad.

Pérdida de reputación

No solo los empleados se sentirán más inseguros y los clientes podrían dejar de serlo, sino que un ciberataque, en términos generales, siempre lleva implícita una pérdida de reputación. Serán muchos los que cuestionen la capacidad de la empresa para protegerse de este tipo de ataques y pondrán en tela de juicio sus procesos internos.

OSINT

La inteligencia de fuentes abiertas (en inglés, open-source intelligence, también conocido por su acrónimo OSINT) es una metodología multifactorial (cualitativa y cuantitativa) de recolección, análisis y toma de decisiones sobre datos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia. En la comunidad de inteligencia, el término "abiertas" se refiere a fuentes disponibles públicamente, en el sentido de opuestas a fuentes secretas o clandestinas. No está relacionado con software libre o software de fuentes abiertas o inteligencia colectiva. – Open Source Solutions Inc.**(8)**

Enfoque

Considero adecuado para esta investigación dada su naturaleza dar un enfoque epistemológico cualitativo, utilizando tres distintos métodos, como hermenéuticos, fenomenológicos y de recolección de información.

Metodología

En ésta investigación se utilizaron técnicas de análisis de *OSINT,* según OSS**(8)** se define como "Una metodología multifactorial de recolección, análisis y toma de decisiones sobre datos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia.", estas fuentes se pueden dividir en seis categorías principales, las cuales son**(9)**:

- **Medios de comunicación:** periódicos, revistas, emisoras de radio y cadenas de televisión;
- **Internet:** publicaciones en línea, blogs, grupos de discusión, medios ciudadanos (como vídeos grabados con teléfono móvil y contenidos creados por usuarios), YouTube y redes sociales (como Facebook, Twitter o Instagram).
- **Datos gubernamentales:** informes, presupuestos, audiencias, guías telefónicas, conferencias de prensa, mítines, discursos y sitios web gubernamentales.
- **Publicaciones profesionales y académicas:** información sacada de revistas académicas, conferencias, simposios, disertaciones y tesis.
- **Datos comerciales:** imágenes comerciales, evaluaciones financieras e industriales y bases de datos.
- **Literatura gris:** informes técnicos, preimpresiones, patentes, documentos de trabajo, documentos comerciales, trabajos inéditos y boletines.

En este caso nos centraremos en dos principalmente, medios de comunicación e internet como fuentes de información primarias

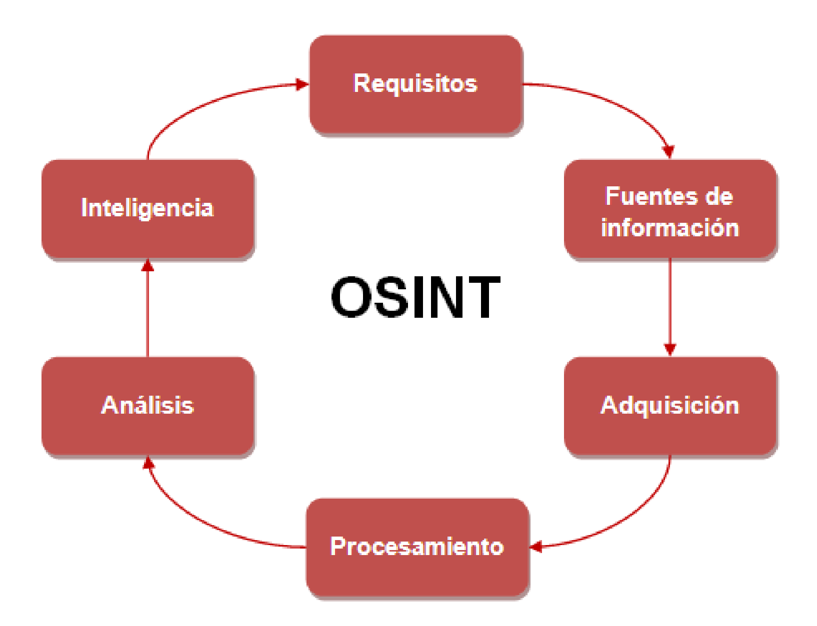
Como herramienta principal se utilizaron los parámetros de búsqueda avanzada de google, al ser el más popular motor de búsquedas global nos provee de una enorme cantidad de resultados, pero con la ayuda de sus filtros de búsqueda podemos encontrar información muy específica, he aquí un ejemplo de su funcionamiento:

inurl:”ues.edu.sv/” intext:biblioteca

Primero especificamos una serie de caracteres que se encuentran en el hiperenlace, luego especificamos una cadena de texto que se debe encontrar en el sitio.

Ciclo de inteligencia

Logramos efectuar la investigación con la metodología usada en el ciclo de inteligencia, que se representa de forma gráfica a continuación **(10)**:



Primero definimos el problema, también planteamos los objetivos e hipótesis.

Luego identificamos fuentes de información para luego pasar a el proceso de adquisición de

forma ordenada y procesar esos datos logrando dar pie a un análisis lógico de la información obtenida.

Ya hecho el análisis podemos generar un reporte de inteligencia y satisfacer los requisitos establecidos al principio.

Técnicas de Investigación

Fuentes de información:

Parámetros de búsquedas avanzadas en el buscador web Google.

https://www.zone-h.org/ / Sitio dedicado a documentar y respaldar información relacionada a los defaces web en el mundo.

Sitios de verificación de credenciales comprometidas:

Have i been pwned: https://haveibeenpwned.com/

Dehashed: https://dehashed.com/

Intelligence X: https://intelx.io/

Pwndb: http://pwndb2am4tzkvold.onion

Red social Facebook.

Adquisición:

De acuerdo con algunos estudiantes del Alma Máter, al entrar al expediente las notas de la carga académica correspondientes al ciclo 01 de este 2020 habían sido modificadas con la nota 6.90 en todas las materias. Asimismo, al ingresar a la página web de la biblioteca universitaria, los estudiantes se encontraban con fallas y no lograban entrar al sistema **(1)**.

Comenzamos con una nota publicada por elsalvador.com en:

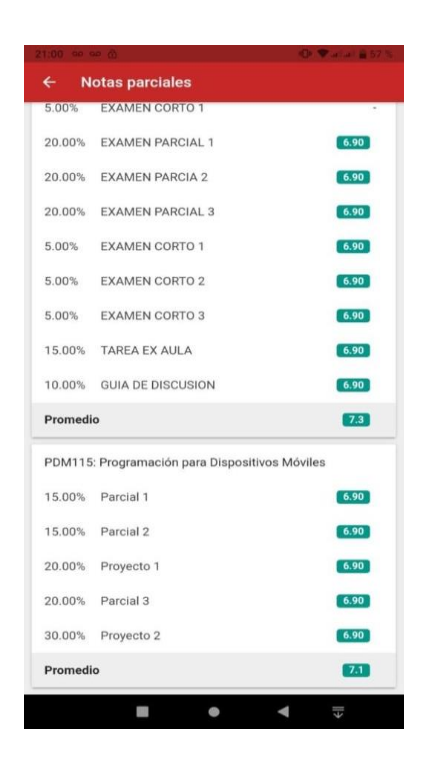
https://www.elsalvador.com/noticias/nacional/hackean-sistema-web-universidad-el-salvador/732239/2020/

En un audio compartido por la fuente, Azcúnaga explica que “al parecer fueron unas actualizaciones que han generado esa situación y están tratando de recuperar lo que ya estaba introducido en el sistema (las notas) y se podrá visualizar”.

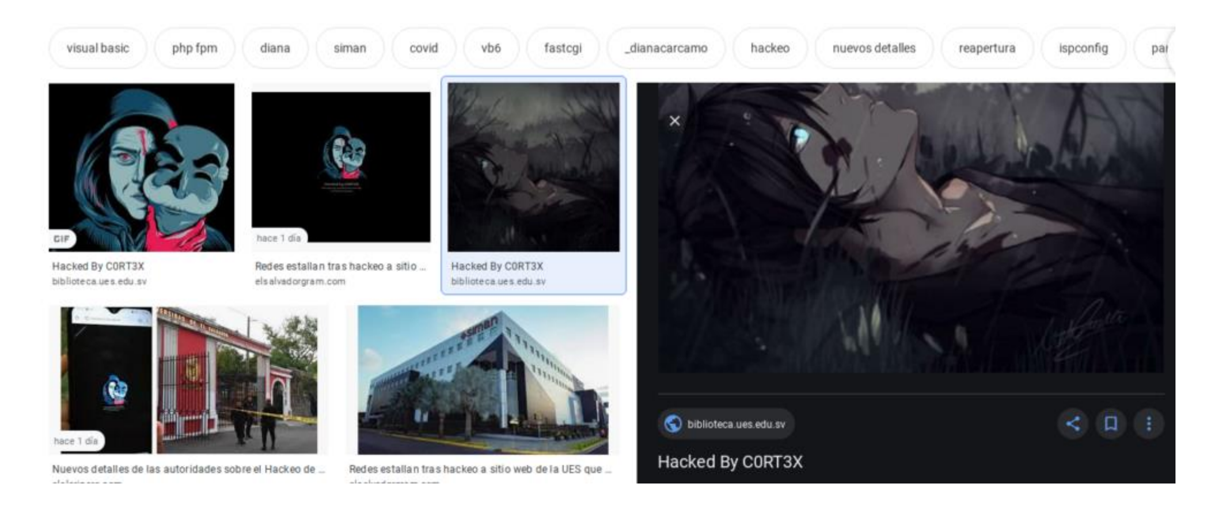
“Bien raro que ni a los correos institucionales de cada empleado de la UES, autoridades ni los encargados del sistema hayan avisado que el sistema presentaría problemas, no

explican qué pasa y para cuándo estará arreglado. Eso hace pensar que no quieren admitir el hackeo del sistema”, mencionó un docente de la UES.

“Este 15 de julio, estaba programado como último día de introducir notas al sistema Prometeo y para los docentes que aún no han terminado, esperamos que den prórroga, ya por segundo día y nada claro” añadió.



Seguidamente se realiza una búsqueda en google “inurl:biblioteca.ues.edu.sv “c0rt3x””



Al parecer según ésta imagen C0RT3X tiene interés por la animación japonesa.

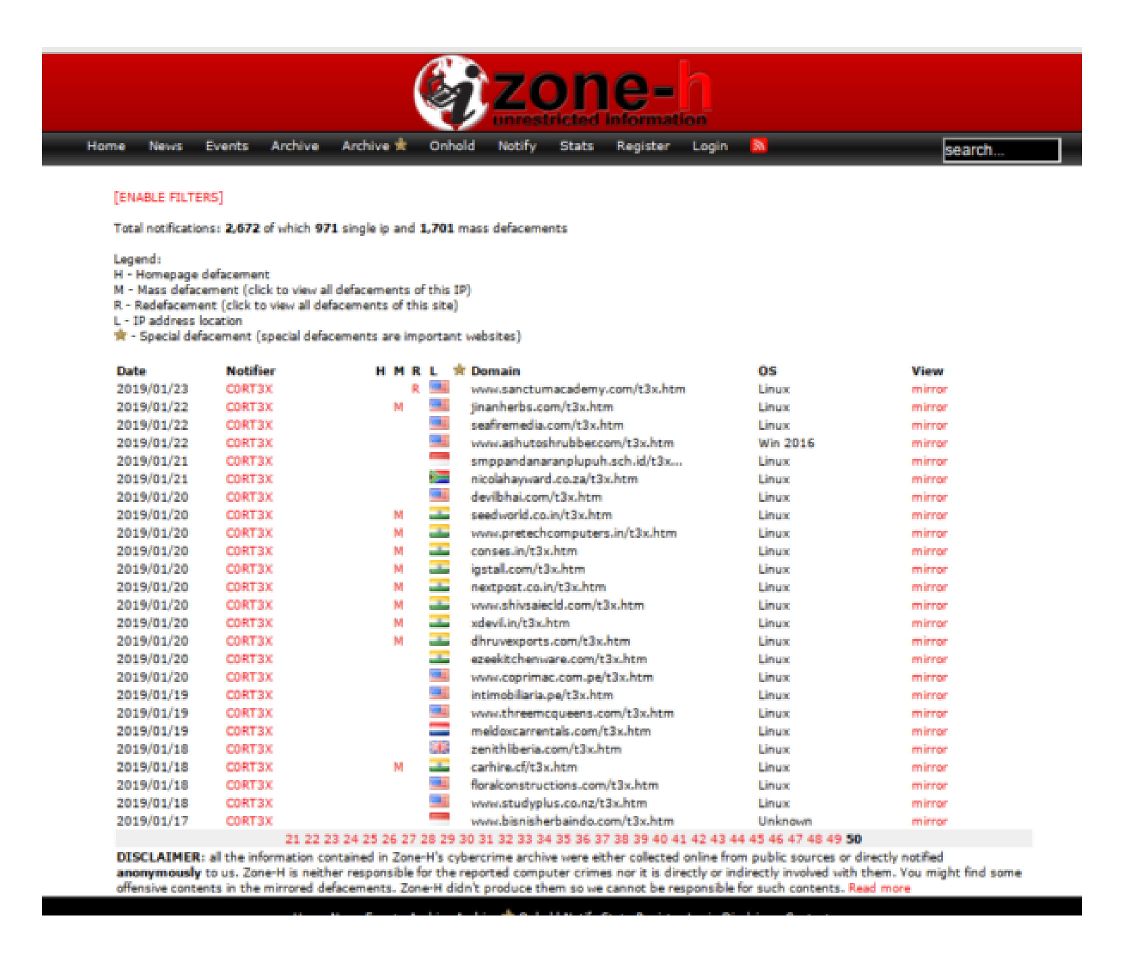
La página web de la biblioteca se encontraba así:



Las modificaciones hechas al sitio dejan dos cuestiones en evidencia:

- Pertenece a un grupo o asociación de hackers llamada «Pacman Corp».
- El individuo no tiene buen dominio del inglés o ha utilizado el traductor para dejar su lema en la página, ya que no tiene ninguna lógica «The university is as bad as the university», el texto no posee una Buena sintáxis.

Ahora nos dirigimos al sitio zone-h para comprobar los registros de la actividad de C0RT3X, que muestra que lleva contabilizado desde 2019 de forma official más de 2,600 notificacines.
https://archive.is/o/Bcn0K/https://zone-h.net/archive/notifier=C0RT3X/page=50



[ENABLE FILTERS]

Total notifications: **2,672** of which **971** single ip and **1,701** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2019/01/23	CORT3X			R			www.sanctumacademy.com/t3x.htm	Linux	mirror
2019/01/22	CORT3X		M				jinanherbs.com/t3x.htm	Linux	mirror
2019/01/22	CORT3X						seafiremedia.com/t3x.htm	Linux	mirror
2019/01/22	CORT3X						www.ashutoshrubber.com/t3x.htm	Win 2016	mirror
2019/01/21	CORT3X						smppandanaranplupuh.sch.id/t3x...	Linux	mirror
2019/01/21	CORT3X						nicolahayward.co.za/t3x.htm	Linux	mirror
2019/01/20	CORT3X						devilbhai.com/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				seedworld.co.in/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				www.pretechcomputers.in/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				conses.in/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				igstall.com/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				nextpost.co.in/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				www.shivsaiecld.com/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				xdevil.in/t3x.htm	Linux	mirror
2019/01/20	CORT3X		M				dhruvexports.com/t3x.htm	Linux	mirror
2019/01/20	CORT3X						ezeekitchenware.com/t3x.htm	Linux	mirror
2019/01/20	CORT3X						www.coprimac.com.pe/t3x.htm	Linux	mirror
2019/01/19	CORT3X						intimobiliaria.pe/t3x.htm	Linux	mirror
2019/01/19	CORT3X						www.threemcqueens.com/t3x.htm	Linux	mirror
2019/01/19	CORT3X						meldoxcarrentals.com/t3x.htm	Linux	mirror
2019/01/18	CORT3X						zenithliberia.com/t3x.htm	Linux	mirror
2019/01/18	CORT3X		M				carhire.cf/t3x.htm	Linux	mirror
2019/01/18	CORT3X						floralconstructions.com/t3x.htm	Linux	mirror
2019/01/18	CORT3X						www.studyplus.co.nz/t3x.htm	Linux	mirror
2019/01/17	CORT3X						www.bisnisherbaindo.com/t3x.htm	Unknown	mirror

21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 **50**

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Podemos notar entre otras cosas aparte del gran número de defaces es que ha comprometido varios sitios .gov, además de que todos sus defaces tienen la misma estructura, una imagen, su firma personal y con la de compañeros de su grupo, raramente se le ve firmando solo una página web, deja un medio de contacto y lo más importante de tdo es que siempre el deface va en un archive html llamado “t3x.htm” algo que no se nota en el hackeo a la UES .

He aquí un ejemplo de un deface:

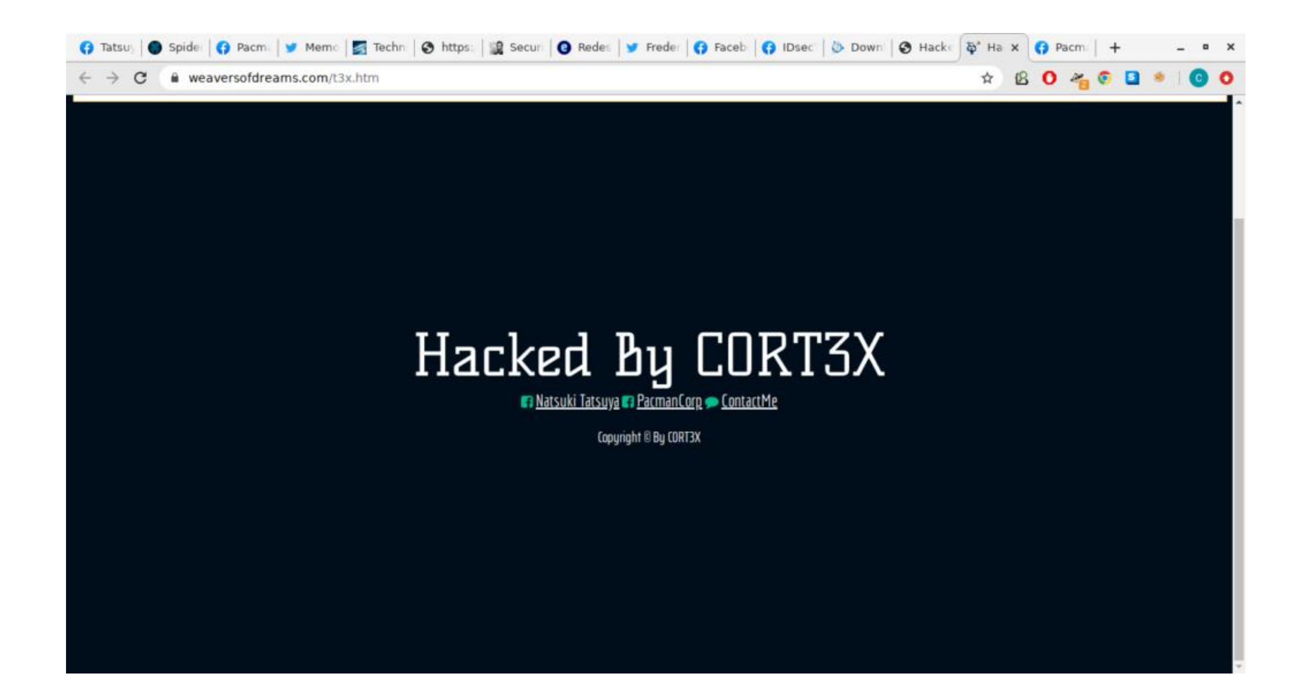


En la adquisición de información logré recopilar algunos emails utilizados:

- kanghaxor@gmail.com
- c0rt3x021@gmail.com
- ryuukatsumi21@gmail.com

Intenté hacer uuso de distintas herramientas para comprobar si algún email había sido expuesto en alguna filtración de datos pero la búsqueda fué infructuosa, si se hubiera logrado obtener información arroaria datos como contraseñas, sitios en los que se ha registrado, direcciones IP, et.

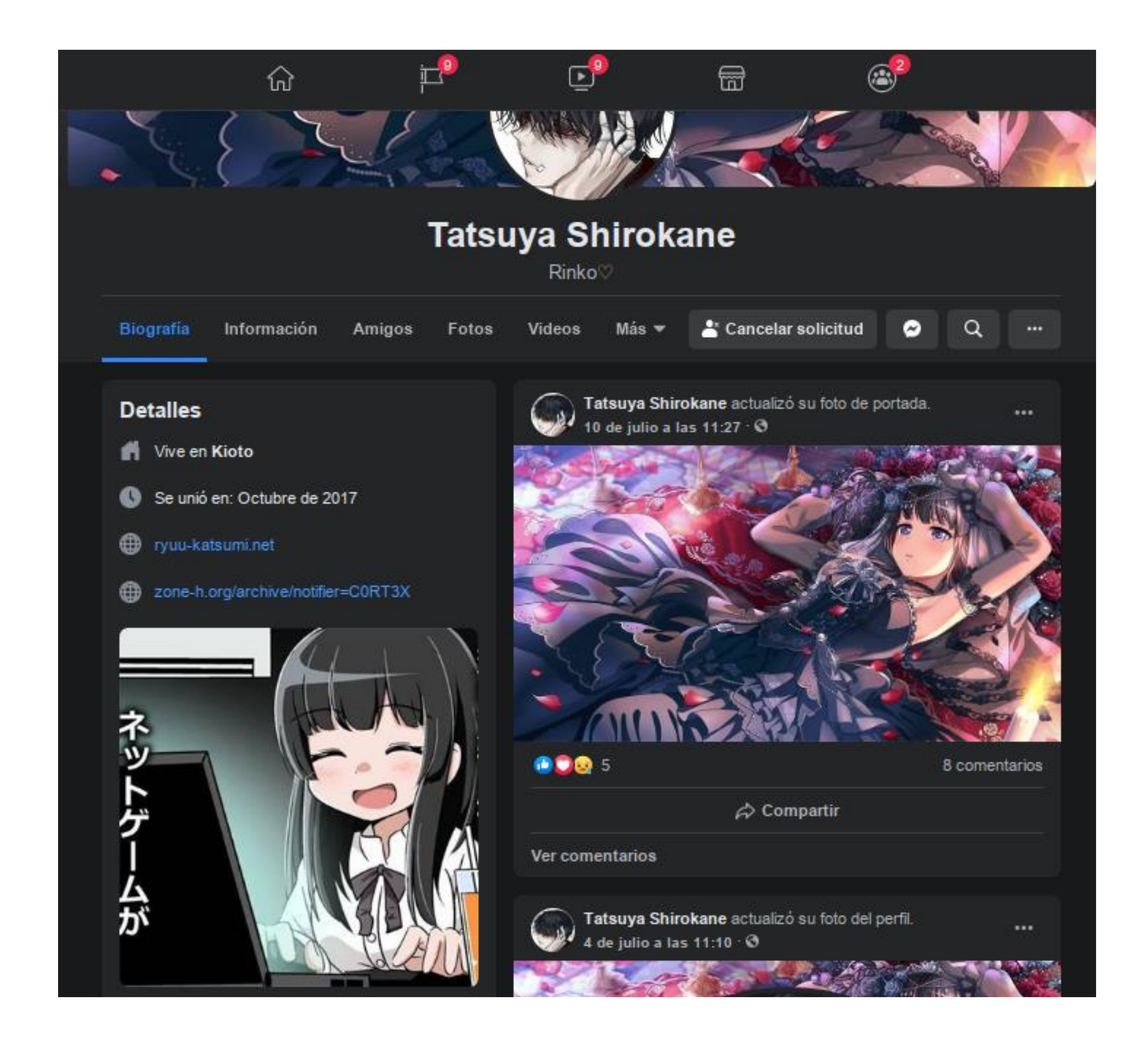
Hay varios defaces que hacen conexión a sus redes sociales y las de su grupo, las cuales no tienen muchos seguidores y además claramente se ve que están administradas por personas que viven en Indonesia.



He aquí la lista de redes que conseguí:

- Sitio web oficial de PacmanCorp: https://www.facebook.com/OfficialPacmanCorpTeam
- IDsecTeam Official: http://facebook.com/IDsecTeam-Official-401667713575598/
- Y para finalizar el facebook oficial de c0rt3x que se correlaciona en uno de sus defaces: https://www.facebook.com/cortex.jp

Lo más importante es el perfil personal de él:



Obtenemos información como su fecha de registro en facebook, octubre de 2017, enlace de su blog personal y un enlace a su perfil de zone-h.org.

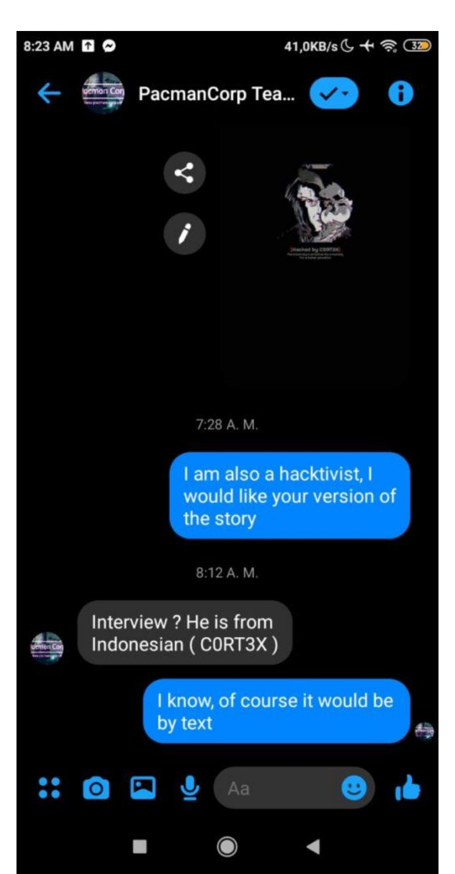
Revisando entre sus fotos de perfil, encontré esta, subida el 3 de enero, hice una búsqueda inversa infructuosa, que confirma que la imagen ha sido subida sólo por él, he aquí C0RT3X:

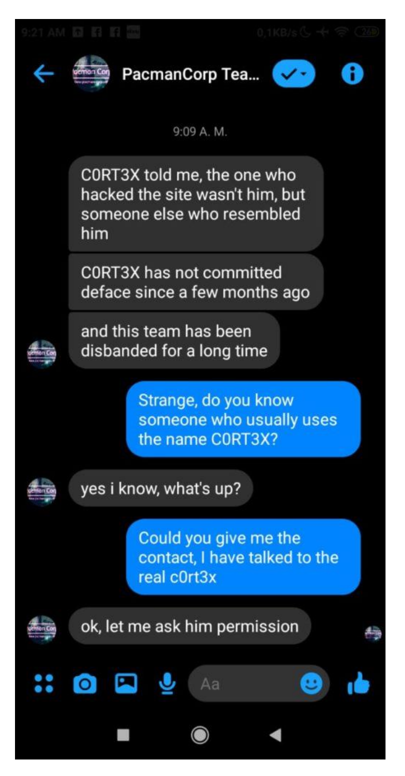
https://scontent.fsal2-1.fna.fbcdn.net/v/t1.6435-9/175563703_930225127743645_4187689205334860756_n.jpg?_nc_cat=111&ccb=1-3&_nc_sid=174925&_nc_ohc=AjrXvh_sLTgAX8evSR4&_nc_oc=AQmM5KK1UY53ZfB4BZY8iRGM-cmIo0nvWvYRNpXEfe7j915aPfVsxHuZ-b6sz4EOd1A&_nc_ht=scontent.fsal2-1.fna&oh=eb387805dbfe489afc450a66af5263a0&oe=60D3F375



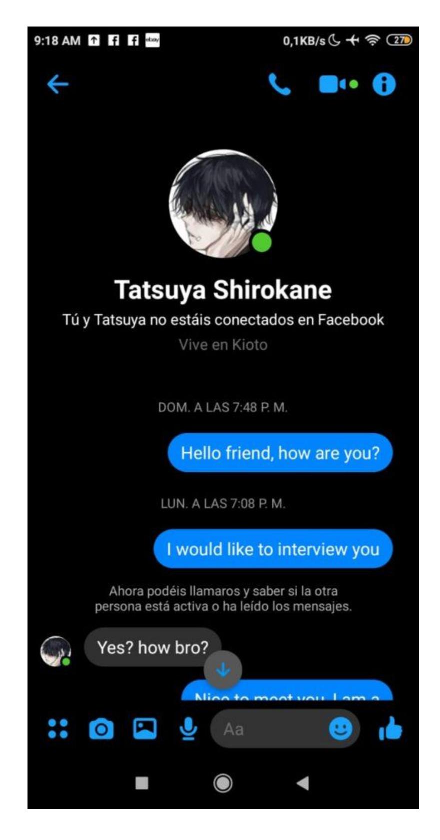
Logré entrevistar brevemente al administrador de la página official del grupo hacktivista primero:

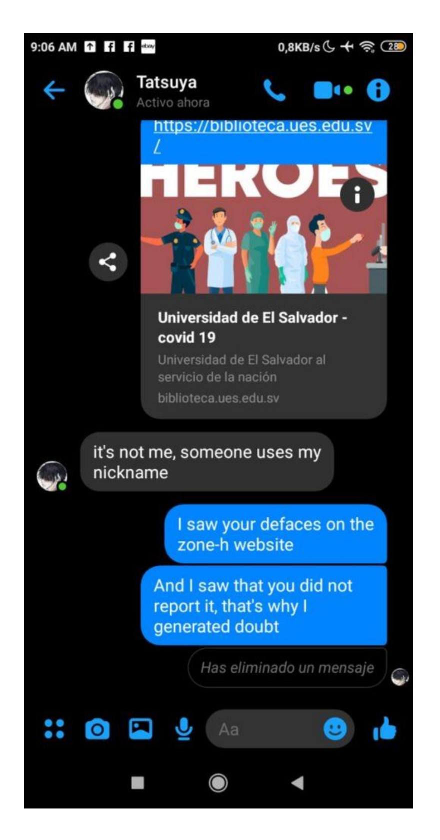


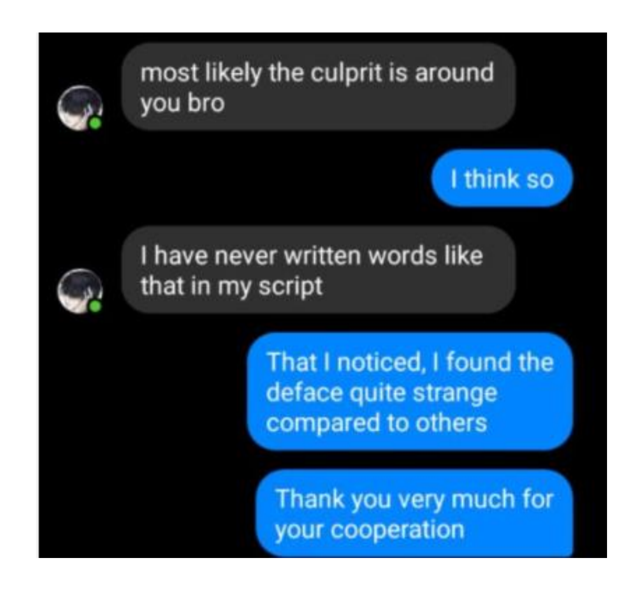


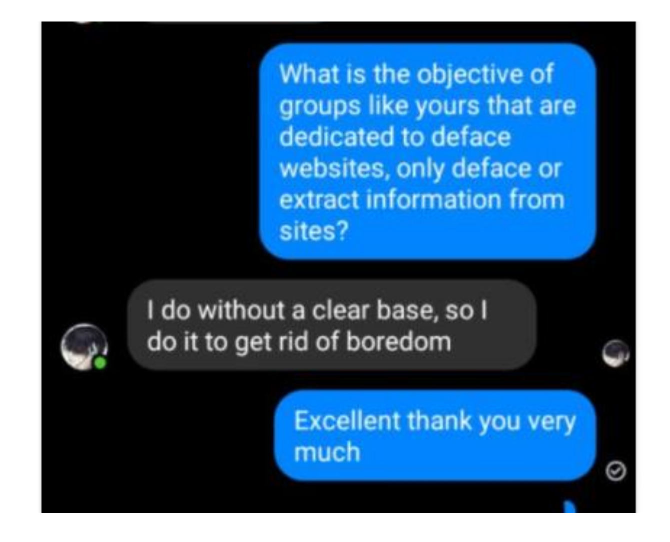


Bien, confirmamos algunas cosas, primero que C0RT3X vive en Indonesia, que C0RT3X asegura no ser el autor del deface, que alguien está suplantando su identidad, que lleva algún tiempo sin realizar defaces y que además el equipo de hackers lleva desmantelado algún tiempo, ahora veamos qué dice el hacker C0RT3X:









Al finalizar nuestra coversación le hice la siguiente pregunta:

¿Cuál es el objetivo de los grupos como el tuyo dedicados a defacear sitios web, sólo defacearlos o extraer información de ellos?

A lo que me respondió:

Lo hago sin objetivos claros, lo hago sólo para matar el aburrimiento.

No parece que un ataque sofisticado que tuviera como objetivo el sistema Prometeo fuera vulnerado por una persona como ésta.

Inteligencia

Teniendo en cuenta los patrones de ccomportamiento de C0RT3X a la hora de realizer ataques, entre ellos:

- Atribuirse oficialmente un deface.
- Vincular un correo electrónico o su perfil en la red social facebook.
- Subir el deface en un archivo tex.htm.
- Cuando se hace mención de se grupo deja las firmas de los demás integrantes.
- No profundiza en los sitios web comprometidos.
- No deja ese tipo de frases plasmadas en los sitios web.
- Ocasionalmente hace referencia a la animación japonesa en sus defaces.

Además desde las páginas oficiales se nos dice que elk grupo había sido desmantelado hace tiempo.

Y el hackeo tuvo un impacto politico en la realidad naciona como podemos notar en el comunicado official de la ues en el sitio:





Lo que puede dar a enteder que alguien suplantó la identidad de C0RT3X para pasar desapercibido ante la vista pública, pero no comprendía el modo operative de C0RT3X lo cual deja en evidencia el actuar el día 11 de julio, ésta persona tenia como finalidad utilizar este evento para llamar la atención del gobierno por el pago adeudado en aquel entonces, posiblemente sea una persona que trabaje dentro de la institución.

Cronograma

Cronograma del mes de Julio

El siguiente diagrama de Gantt nos ayuda a visualizar de manera cronológica el ciclo de investigación durante el mes de Julio a partir del día sábado 11

	11	12	13	14	15	16
Sitio web comprometido	✓					
Recopilación de datos	✓	✓	✓	✓	✓	✓
Contacto con PacmanCorp		✓				
Entrevista a CORT3X			✓			
Emisión de Comunicado UES		✓				

Bibliografía

(1) Cecilia Fuentes, C. F. (2020, 12 julio). Hackean páginas web de la Universidad de El Salvador y cambian a 6.90 las notas de los alumnos. elsalvador.com. https://www.elsalvador.com/noticias/nacional/hackean-sistema-web-universidad-el-salvador/732239/2020/

(2) Aguilar, L. D., & Aguilar, L. D. (2020, 30 agosto). ¿Qué son los «defacements»? Derecho de la Red. https://derechodelared.com/que-son-los-defacements/

(3) Trendmicro. (s. f.). Website Defacement. Recuperado 27 de mayo de 2021, de https://www.trendmicro.com/vinfo/us/security/definition/website-defacement

(4) INCIBE. (2021, 16 abril). Protégete frente al defacement y que no le cambien la cara a tu web. https://www.incibe.es/protege-tu-empresa/blog/protegete-frente-al-defacement-y-no-le-cambien-cara-tu-web

(5) Deloitte Spain. (2018, 25 junio). Las ciberamenazas ponen en alerta a las universidades. https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciberamenazas-alertan-universidades.html

(6) Accenture. (2016). The State of Cybersecurity and Digital Trust 2016 Identifying Cybersecurity Gaps to Rethink State of the Art [Libro electrónico]. Accenture. https://www.accenture.com/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf

(7) ReasonWhy Spain. (2017, 15 mayo). Qué consecuencias puede tener un ciberataque para tu empresa. ReasonWhy. https://www.reasonwhy.es/actualidad/digital/que-consecuencias-puede-tener-un-ciberataque-para-tu-empresa-2017-05-15

(8) Robert D. Steele, R. S. (2002). NATO OSINT Reader. Open Source Intelligence: What Is It? Why Is It Important to the Military? https://web.archive.org/web/20180328191016/http://www.oss.net/dynamaster/file_archive/040320/fb893cded51d5ff6145f06c39a3d5094/OSS1997-02-33.pdf

(9) Richelson, J. (2016). The U.S. Intelligence Community. Van Haren Publishing.

(10) A. (2017, 24 junio). OSINT para pentest. BCNSoluciona, siempre existe una solución. https://www.bcnsoluciona.com/blog/osint-para-pentest/

Glosario

Sistema PROMETEO: Sistema de Registro Académico Centralizado, que reúne los proceso llevados a cabo por las diferentes unidades académicas y facultades, permite realizar procesos como registro académico, graduaciones, expediente en línea y procesos de gestión financiera, administración, entre otros.

Deface: Es un ataque a un sitio web que cambia la apariencia visual de una página web. Normalmente son producidos por hackers que obtuvieron algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.

Rasomware: Un ransomware, o «secuestro de datos» en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Bitcoin: Bitcoin es un protocolo, proyecto de código abierto y red entre iguales que se utiliza como criptomoneda, sistema de pago y mercancía. Fue concebida en 2008 por una entidad conocida bajo el seudónimo de Satoshi Nakamoto, cuya identidad concreta se desconoce.

Hacktivismo: (acrónimo de hacker y activismo también conocido como ciberactivismo) Se entiende normalmente "la utilización no-violenta de herramientas digitales persiguiendo fines políticos.

Data breach: Es el acceso por partes no autorizadas a datos de acceso restringido. Su peligro existe por la exposición de información y archivos confidenciales a personas no autorizadas sin permiso.